Testimony of
Gerry Keegan
CTIA – THE WIRELESS ASSOCIATION®
In Opposition to Senate Bill 629

February 24, 2015

Before the Connecticut General Assembly General Law Committee

Co-Chairs Leone and Baram and members of the Committee, I am Gerry Keegan with CTIA-The Wireless Association®, the trade association for the wireless communications industry, in opposition to Senate Bill 629. Although the wireless industry shares the sponsor's goal of reducing smartphone theft, we do not support the approach proposed in this bill as we believe it is unnecessary - given the wireless industry's commitment to provide anti-theft tools to consumers - and unworkable.

In April 2014, CTIA and participating wireless companies announced a smartphone anti-theft commitment, which is one of the most recent efforts by the industry to help aid law enforcement to deter smartphone thefts in the United States. In Part I of the Commitment each device manufacturer and operating system signatory agrees that new models of smartphones first manufactured after July 2015 for retail sale in the United States will offer, at no cost to consumers, a baseline anti-theft tool that is preloaded or downloadable on wireless smartphones. Part II of the Commitment provides that each network operator that is a signatory commits to permit the availability and full usability of a baseline anti-theft tool to be pre-loaded or downloaded.

This announcement by the wireless industry negates any need for passing SB 629. The industry has already committed to providing this tool to consumers, which will further strengthen the fight against smartphone theft. The most recent announcement is in addition to a number of steps taken by the wireless industry to assist law enforcement in their efforts to address smartphone theft, including the deployment of an integrated stolen phones database, outreach to educate consumers, and the development of numerous security solutions. This multi-layered approach, which is necessary to truly combat smartphone theft, is absent in this legislation.

CTIA and its member companies have work collaboratively with the Federal Communications Commission (FCC), law enforcement officials, and lawmakers to help prevent smartphone thefts and to dry up the aftermarket for stolen phones. In April 2012, we announced a voluntary commitment by CTIA and participating wireless companies to take certain actions to help law enforcement deter smartphone theft and protect personal data, including the development of a stolen phones database to report and track all stolen 4G/LTE phones in the U.S. All participating wireless carriers completed this database integration in November 2013. Wireless carriers use the database to check whether a smartphone presented to them has been reported lost or stolen. If the smartphone has been reported lost or stolen, it will be denied service on carrier networks.

The database is interconnected across mobile carriers and is a resource for law enforcement to use to deter thefts. To enhance the effectiveness of the database solution, U.S. databases are integrated internationally. Efforts are underway to link more foreign carriers and countries to the database to mitigate the export of stolen phones to markets outside the U.S. In collaboration with carriers, local law enforcement should make extensive use of the industry's stolen, phones database and corresponding solutions. I would like to take this opportunity to invite Connecticut law enforcement agencies to seek access to the database.

In addition to the deployment of the integrated database, the wireless industry has been individually and collectively educating consumers on ways to help reduce smartphone theft. These initiatives include highlighting consumer use of passwords, applications, and other preventative measures so that if a consumer's smartphone is ever lost or stolen, personal information is protected. These education efforts include information at the time of smartphone activation, public service announcements, websites, e-mail, and social media outreach.

CTIA and its members have also taken steps to aid law enforcement by providing resources to educate consumers about measures they can and should take. CTIA developed a website beforeyouloseit.org for tips and information. We also developed an attention grabbing public service

announcement with guidance to consumers to use their smartphones' features and apps to remote lock, track, and wipe their devices if they are lost or stolen. Most recently, CTIA made available business cards in Spanish and English to provide smart tips to consumers to deter smartphone theft.

In addition to being unnecessary in light of these industry commitments, SB 629 suggests that state-by-state regulation is workable in this area. State-by-state regulation will never keep pace with innovation in the global wireless ecosystem. What lawmakers mandate as a solution today may not be - and may interfere with - the solution consumers need tomorrow. Any mandated technology standard will quickly become outdated in the fast paced tech industry. Moreover, requiring a particular technology mandate is counter to the policies that have made the wireless industry one of the most important and vibrant sectors of our economy.

Wireless service operates without regard to state lines and thus is uniquely interstate and national. As the FCC has explained, Congress sought to ensure a "national regulatory policy" for wireless, "not a policy that is balkanized state-by-state." SB 629 will influence device design, manufacturing, and wireless service far beyond Connecticut's borders. And, if other states, territories, and local governments regulate in this area, the potential for conflicting technical and operational requirements among state legislatures, not to mention thousands of local governments, is staggering. The resulting patchwork of state and local laws will negatively impact wireless consumers. Even the most knowledgeable wireless consumers may experience confusion when purchasing and using their devices under those circumstances.

CTIA and wireless companies are committed to continuing to develop solutions to prevent smartphone theft. In June 2014, the Chairman of the FCC convened a workshop on the prevention of mobile device theft. CTIA participated on a panel with law enforcement representatives regarding the nature of the problem and steps that the industry had taken in support of law enforcement efforts. As a result of the workshop, the FCC Chairman chartered the Technological Advisory Committee (TAC) to address a set of recommendations for preventing the theft of mobile devices by the end of 2014.

To fulfill the Chairman's mandate, the TAC created a new working group - the Mobile Device Theft Prevention (MDTP) Working Group. The first organizational meeting of the MDTP took place on August 1, 2014. The group is organized into five areas: problem definition, existing solutions, gap analysis, cybersecurity and privacy, and consumer outreach. The group made over 30 recommendations to the FCC Chairman on December 4, 2014. That report is now out for public comment with the initial comment period ending January 30, 2015. The Connecticut General Assembly should allow the wireless industry to meet its previously announced commitment to provide anti-theft solutions to consumers and allow the process at the federal level to work before considering legislation on this issue.

In closing, the wireless industry has been at the forefront of addressing smartphone theft. The industry's ongoing multi-layered efforts eliminate the need for new legislation on this issue. The approach incorporated in SB 629, although well-intentioned, will lead to unintended negative consequences for Connecticut consumers. For these reasons, we respectfully ask that you not move SB 629. Thank you for your time.

Smartphone Anti-Theft Voluntary Commitment
Released April 15, 2014

Part I

Each device manufacturer and operating system signatory of Part I of this "Smartphone Anti-Theft Voluntary Commitment" agrees that new models of smartphones first manufactured after July 2015 for retail sale in the United States will offer, at no cost to consumers, a baseline anti-theft tool that is preloaded or downloadable on wireless smartphones that provides the connected capability to:

1. Remote wipe the authorized user's data (i.e., erase personal info that is added after purchase such as contacts, photos, emails, etc.) that is on the smartphone in the event it is lost or stolen.
2. Render the smartphone inoperable to an unauthorized user (e.g., locking the smartphone so it cannot be used without a password or PIN), except in accordance with FCC rules for 911 emergency communications, and if available, emergency numbers programmed by the authorized user (e.g., "phone home").
3. Prevent reactivation without authorized user's permission (including unauthorized factory reset attempts) to the extent technologically feasible (e.g., locking the smartphone as in 2 above).
4. Reverse the inoperability if the smartphone is recovered by the authorized user and restore user data on the smartphone to the extent feasible (e.g., restored from the cloud).

In addition to this baseline anti-theft tool, consumers may use other technological solutions, if available for their smartphones.

Part II

Each network operator signatory of Part II to the "Smartphone Anti-Theft Voluntary Commitment" commits to permit the availability and full usability of a baseline anti-theft tool to be preloaded or downloadable on smartphones as specified in this commitment.

###

The following network operators, device manufacturers and operating system companies are participating in the voluntary commitment: Apple Inc.; Asurion; AT&T; Google Inc.; HTC America, Inc.; Huawei Device USA; LG Electronics MobileComm USA, Inc; Motorola Mobility LLC; Microsoft Corporation; Nokia, Inc.; Samsung Telecommunications America, L.P.; Sprint Corporation; T-Mobile USA; U.S. Cellular; Verizon Wireless; and ZTE USA, Inc.

For more information, please visit the Smartphone Anti-Theft FAQ.

CTIA
The Wireless Association®

Expanding the Wireless Frontier

CTIA and Participating Wireless Companies Announce the "Smartphone Anti-Theft Voluntary Commitment"

WASHINGTON, April 15, 2014 – CTIA and participating wireless companies today announced the "Smartphone Anti-Theft Voluntary Commitment," which is the most recent effort by the industry to deter smartphone thefts in the U.S. The safety and security of wireless users remain the wireless industry's top priority, and is why this commitment will continue to protect consumers while recognizing the companies' need to retain flexibility so they may constantly innovate, which is key to stopping smartphone theft. The "Smartphone Anti-Theft Voluntary Commitment" states:

Part I

Each device manufacturer and operating system signatory of Part I of this "Smartphone Anti-Theft Voluntary Commitment" agrees that new models of smartphones first manufactured after July 2015 for retail sale in the United States will offer, at no cost to consumers, a baseline anti-theft tool that is preloaded or downloadable on wireless smartphones that provides the connected capability to:

1. Remote wipe the authorized user's data (i.e., erase personal info that is added after purchase such as contacts, photos, emails, etc.) that is on the smartphone in the event it is lost or stolen.

2. Render the smartphone inoperable to an unauthorized user (e.g., locking the smartphone so it cannot be used without a password or PIN), except in accordance with FCC rules for 911 emergency communications, and if available, emergency numbers programmed by the authorized user (e.g., "phone home").

3. Prevent reactivation without authorized user's permission (including unauthorized factory reset attempts) to the extent technologically feasible (e.g., locking the smartphone as in 2 above).

4. Reverse the inoperability if the smartphone is recovered by the authorized user and restore user data on the smartphone to the extent feasible (e.g., restored from the cloud).

In addition to this baseline anti-theft tool, consumers may use other technological solutions, if available for their smartphones.

Part II

Each network operator signatory of Part II to the "Smartphone Anti-Theft Voluntary Commitment" commits to permit the availability and full usability of a baseline anti-theft tool to be preloaded or downloadable on smartphones as specified in this commitment.

The following network operators, device manufacturers and operating system companies are participating in the voluntary commitment: Apple Inc.; Asurion; AT&T; Google Inc.; HTC America, Inc.; Huawei Device USA; LG Electronics MobileComm USA, Inc.; Motorola Mobility LLC; Microsoft Corporation; Nokia, Inc.; Samsung Telecommunications America, L.P.; Sprint Corporation; T-Mobile USA; U.S. Cellular; and Verizon Wireless.

"We appreciate the commitment made by these companies to protect wireless users in the event their smartphones are lost or stolen. This flexibility provides consumers with access to the best features and apps that fit their unique needs while protecting their smartphones and the valuable information they contain. At the same time, it's important different technologies are available so that a 'trap door' isn't created that could be exploited by hackers and criminals," said Steve Largent, President and CEO, CTIA.

"By working together with policymakers, law enforcement and consumers, we will deter theft and protect users' personal information on smartphones."

Oregon State Senator Bruce Starr, President of the National Conference of State Legislatures (NCSL), said, "The NCSL applauds today's announcement unveiling the wireless industry's commitment to reduce the number of smartphone thefts each year by providing anti-theft tools on future devices. This voluntary effort serves as another positive illustration of the wireless industry adapting to address consumer needs through self-regulation. The NCSL encourages your ongoing collaboration with consumers and the state lawmakers as we continue to work cooperatively to reduce the number of smartphone thefts annually."

"While the Minnesota legislature is poised to pass the nation's first 'kill switch' law as early as next week, I have said all along we would welcome the industry's ideas and solutions to address this critical public safety issue. With today's announcement, CTIA and its member companies have stepped up to protect customers and promote public safety, and I commend and support their efforts," said Minnesota State Representative Joe Atkins.

"I am encouraged by these steps to deter smartphone thefts and hopeful that that these measures will bring much needed protections to Chicago consumers," said Chicago Alderman Edward M. Burke. "As the sponsor of pending legislation that seeks to mandate 'kill switch' technology on all smartphones sold in Chicago, I commend the smartphone industry for its cooperative efforts, but will remain watchful that these commitments are both upheld and result in the shared goal of reducing smartphone thefts citywide."

"We got the kill switch technology solution we wanted to protect Illinois consumers. The wireless industry has agreed to provide a free preloaded or downloadable anti-theft application for smartphones to help protect owners if their phones are stolen. This tool would allow smartphone owners to remotely wipe their personal data and remotely shut down a stolen phone so it is not valuable to thieves. Today's announcement is a significant step to provide additional protections to Illinois consumers," said Illinois State Senator Toi Hutchinson.

Rhode Island State Senate Majority Leader Dominick J. Ruggerio praised the voluntary commitment by saying, "I am grateful to the participating carriers, device manufacturers and operating system companies for voluntarily coming to this decision to improve public safety. This is a move which is good for consumers and good for business, in my opinion. It gives consumers peace of mind and protects them from the threat of having their personal information exposed. The ability to make the system inoperable also eliminates much of the incentive for theft in the first place."

"Smartphone theft is a growing concern around the country. That's why we introduced legislation to try to stop the secondhand market for stolen smartphones. This agreement will go a long way towards reducing the secondhand market for phones that are stolen, and I commend the industry for taking these steps," said Minnesota State Senator Katie Sieben.

The "Smartphone Anti-Theft Voluntary Commitment" furthers the multi-layered approach previously announced to protect consumers and aid law enforcement. This proactive initiative includes blacklist databases, consumer education and federal legislation (S. 1070), sponsored by U.S. Senator Charles Schumer, to impose tough penalties against those caught stealing devices or modifying them illegally.

###

Phone thefts drop as kill switches become more common

By John Wildermuth and Michael Cabanatuan Updated 9:00 pm, Tuesday, February 10, 2015

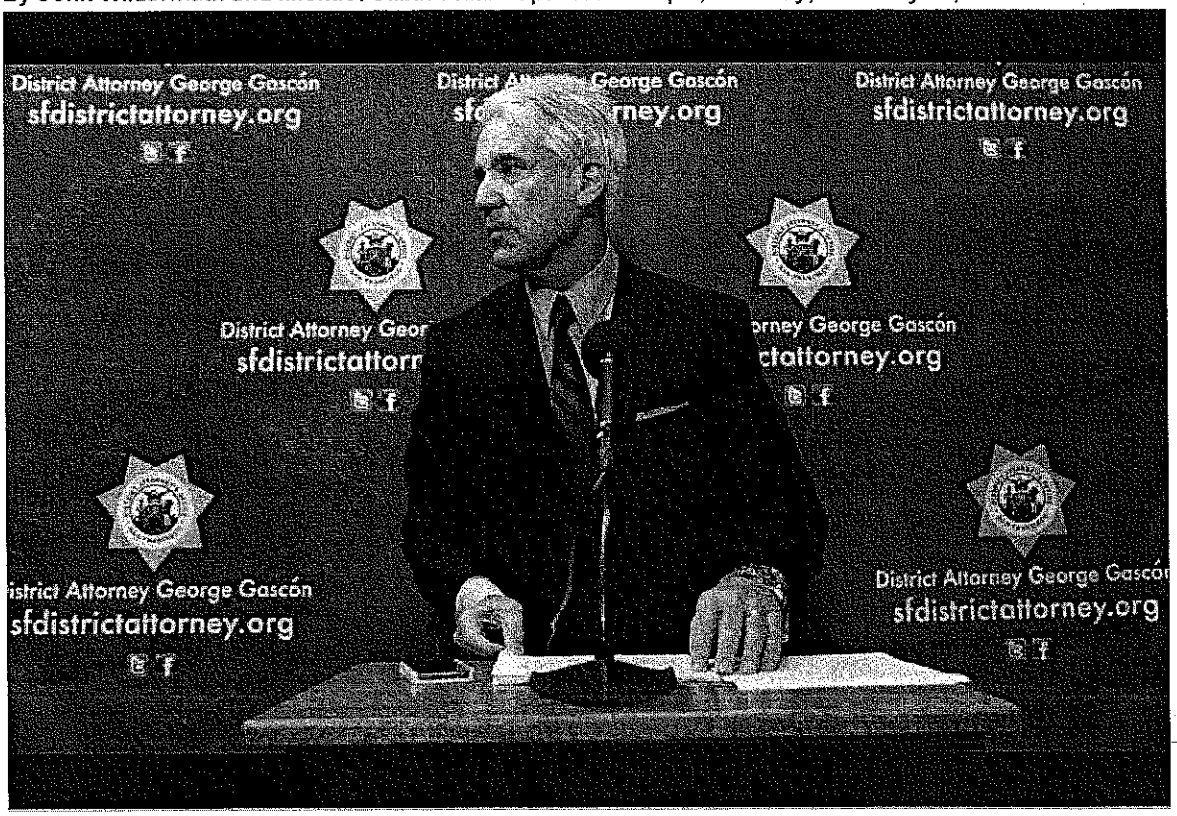

IMAGE 1 OF 2

San Francisco District Attorney George Gascon announces a civil consumer protection action against Uber on Dec. 9.

Smartphone thefts have dropped dramatically in San Francisco and at least two other major cities since "kill switches" started appearing in more cell phones, said District Attorney George Gascón, who has pushed the change.

"The wireless industry continues to roll out sophisticated new features, but preventing their ow customers from being the target of violent crime is the coolest technology they can bring to market," he said in a statement.

The number of smartphone robberies in San Francisco dropped 27 percent in 2013-14, greater than the 22 percent overall drop in robberies. Gascón attributes the change to a strong worldwide push for the inclusion of kill switches in all new phones, which allows stolen phones to be remotely disabled and made useless.

In August, Gov. Jerry Brown signed SB962, a bill requiring all smartphones sold in California after July 1 to contain kill switches, but technology companies already are moving to meet the requirement nationwide.

Apple's kill switch, called Activation Lock, was introduced in September 2013 and is now standard in its new iPhone 6 and 6 Plus. Samsung's Galaxy S5 has had a kill switch since April, and both Microsoft and Goggle plan to include kill switches in their next software updates.

Along with New York Attorney General Eric Schneiderman, Gascón is co-chair of the Secure Our Smartphones Initiative, which has called on wireless companies to adopt kill switches worldwide.

"The huge drops in smartphone theft that have occurred since the kill switch has been on the market are evidence that our strategy is making people safer in our cities and across the world," Schneiderman said in a statement.

So far, it seems to be working. In New York City, cell-phone thefts are down 16 percent, Schneiderman said, and 40 percent in London, according to Mayor Boris Johnson.

—John Wildermuth

Safer streets: Despite the creation of Vision Zero last year — the traffic safety program aimed at eliminating pedestrian and traffic deaths by 2024 — San Francisco still had 29 vehicle-related fatalities, a total that's way too high, a report released by safety activists Tuesday concludes.

Mayor Ed Lee released his own report — a Vision Zero strategy for the next two years — and started a safety training program for professional drivers who operate large vehicles on city streets.

The Vision Zero Coalition, a group of 35 community organizations, in its first progress report, credits the city with adopting the Vision Zero strategy and committing to the ambitious 2024 goal. It says the city's successes include identifying the most dangerous intersections, targeting 24 for improvements by July 1 — nine have been completed — and stepping up enforcement an education.

The progress report also recommends three strategies for 2015, including speeding up safety work on 18 miles of the city's deadliest streets, working for changes in state law to allow automated enforcement of speeding, and focusing enforcement of the five most dangerous traffic behaviors and at the five worst locations.

"We urge the city to continue to act with urgency," the coalition report said. "This means prioritizing safety every step of the way whether deciding the design of a street or where to put limited enforcement resources."

The mayor's "action strategy" calls for similar actions, including focusing enforcement on the same five locations and behaviors, and getting state approval for automated speed enforcement making 13 miles of improvements each year on the most dangerous streets and corridors; and collecting and publicizing a broad range of data about traffic safety, fatalities and injuries.

The training program for large-vehicle drivers is a video-based project that will be required of al Municipal Transportation Agency drivers of large vehicles in future contracts and offered to other professional drivers who operate on city streets.

— Michael Cabanatuan

E-mail: cityinsider@sfchronicle.com Twitter: @sfcityinsider